

IRREDUCIBLE BOOLEAN FUNCTIONS

MONCEF BOUAZIZ¹, MIGUEL COUCEIRO², AND MAURICE POUZET³

ABSTRACT. This paper is a contribution to the study of a quasi-order on the set Ω of Boolean functions, the *simple minor* quasi-order. We look at the join-irreducible members of the resulting poset $\tilde{\Omega}$. Using a two-way correspondence between Boolean functions and hypergraphs, join-irreducibility translates into a combinatorial property of hypergraphs. We observe that among Steiner systems, those which yield join-irreducible members of $\tilde{\Omega}$ are the -2 -monomorphic Steiner systems. We also describe the graphs which correspond to join-irreducible members of $\tilde{\Omega}$.

1. INTRODUCTION

Two approaches to define properties of Boolean functions have been considered in recent years; one in terms of functional equations [10], and one other in terms of relational constraints [19]. As it turned out, these two approaches have the same expressive power in the sense that they specify exactly the same classes (or properties) of Boolean functions. The characterization of these classes was first obtained by Ekin, Foldes, Hammer and Hellerstein [10] who showed that equational classes of Boolean functions can be completely described in terms of a quasi-ordering \leq of the set Ω of all Boolean functions, called *identification minor* in [10, 15], *simple minor* in [19, 7, 4, 5], *subfunction* in [23], and *simple variable substitution* in [2]. This quasi-order can be described as follows: for $f, g \in \Omega$, $g \leq f$ if g can be obtained from f by identification of variables, permutation of variables or addition of dummy variables. As shown in [10], equational classes of Boolean functions coincide exactly with the initial segments $\downarrow K = \{g \in \Omega : g \leq f, \text{ for some } f \in K\}$ of this quasi-order, or equivalently, they correspond to antichains A of Boolean functions in the sense that they constitute sets of the form $\Omega \setminus \uparrow A$. Similarly, those equational classes definable by finitely many equations were shown to correspond to finite antichains of Boolean functions. Since then, several investigations have appeared in this direction, to mention a few, see [2, 3, 11, 19, 20].

This correspondence to function class definability led to a greater emphasis on this quasi-ordering \leq [7, 4, 5, 6]. As any quasi-order, the simple minor relation \leq induces a partial order \sqsubseteq on the set $\tilde{\Omega}$ made of equivalence classes of Boolean functions. Several properties of the resulting poset $(\tilde{\Omega}, \sqsubseteq)$ were established in [7] where a classification of this poset was given in terms of equimorphism (two

¹Institut Supérieur des Technologies Médicales de Tunis, ²University of Luxembourg, ³Université Claude-Bernard Lyon1

Date: February 2, 2008.

2000 *Mathematics Subject Classification.* Combinatorics (05C75), (05C65), (05B05), (05B07), Order, lattices, ordered algebraic structures (06A07), (06E30), Information and communications, circuits (94C10).

Key words and phrases. Boolean function, minor quasi-order, hypergraph, designs, Steiner systems, monomorphy.

The research of the first and last author has been supported by CMCU Franco-Tunisien "Outils mathématiques pour l'informatique".

posets are *equimorphic* if they are equivalent w.r.t. embeddings). Essentially, it was shown that $(\tilde{\Omega}, \sqsubseteq)$ has a sort of universal property among countable posets.

In this paper we are interested in the join-irreducible members of the poset $(\tilde{\Omega}, \sqsubseteq)$, that is, those equivalence classes having a unique lower cover in $(\tilde{\Omega}, \sqsubseteq)$. More precisely, we consider the problem of determining the join-irreducibles of this poset. Rather than taking a direct approach by looking into $(\tilde{\Omega}, \sqsubseteq)$, we attack this problem by looking at hypergraphs. Indeed, the fact that every Boolean function can be represented by a unique multilinear polynomial over the two-element field $GF(2)$ allows to establish a complete correspondence between Boolean functions and hypergraphs. This correspondence is given as follows. For any hypergraph $\mathcal{H} = (V, \mathcal{E})$ we associate the polynomial $P_{\mathcal{H}} \in GF(2)[x_i, i \in V]$ given by $P_{\mathcal{H}} = \sum_{E \in \mathcal{E}} \prod_{i \in E} x_i$. Conversely, every polynomial $P \in GF(2)[x_i, i \in V]$ is of the form $P = P_{\mathcal{H}}$ where $\mathcal{H} = (V, \mathcal{E})$ and \mathcal{E} is the set of hyperedges corresponding to the monomials of P .

To work in complete analogy with the Boolean function setting, we still need to mimic the simple minor relation in the realm of hypergraphs. This is achieved through the notion of quotient map. Say that a map $h': V' \rightarrow V$ is a *quotient map* from $\mathcal{H}' = (V', \mathcal{E}')$ to $\mathcal{H} = (V, \mathcal{E})$ if for every $E \subseteq V$, $E \in \mathcal{E}$ if and only if $|\{E' \in \mathcal{E}' : h'(E') = E\}|$ is odd. For two hypergraphs \mathcal{H}' and \mathcal{H} , set $\mathcal{H} \preceq \mathcal{H}'$ if there is a quotient map from \mathcal{H}' to \mathcal{H} . As we are going to see \preceq constitutes a quasi-order between hypergraphs and two hypergraphs are related by \preceq if and only if the corresponding Boolean functions are related by \leq (see Lemma 9 and Theorem 10, resp.). The fact that a Boolean function (or more accurately an equivalence class) is join-irreducible translates to a combinatorial property of the corresponding hypergraph. A description of all hypergraphs satisfying this property eludes us. But, as we will observe, among these hypergraphs some have been intensively studied for other purposes. The basic examples are the non-trivial hypergraphs whose automorphism group is 2-set transitive. We show that Steiner systems which yield join-irreducible members of the poset $(\tilde{\Omega}, \sqsubseteq)$ are exactly those which are *-2-monomorphic* in the sense that the induced hypergraphs obtained by deleting any pair of two distinct vertices are isomorphic (Theorem 14). Among Steiner triple systems those with a flag-transitive automorphism group enjoy this property. We do not know if there are other. We also describe those graphs corresponding to join-irreducible members of $(\tilde{\Omega}, \sqsubseteq)$ (Theorem 22).

2. BOOLEAN FUNCTIONS

A *Boolean function* is simply a mapping $f: \{0, 1\}^n \rightarrow \{0, 1\}$ where $n \geq 1$ and called the *arity* of f . The simplest examples of n -ary Boolean functions are the *projections*, i.e., mappings $(a_1, \dots, a_n) \mapsto a_i$, for $1 \leq i \leq n$ and $a_1, \dots, a_n \in \{0, 1\}$, and which we also refer to as *variables*. For each $n \geq 1$, we denote by $\Omega^{(n)} = \{0, 1\}^{\{0, 1\}^n}$ the set of all n -ary Boolean functions and we denote by $\Omega = \bigcup_{n \geq 1} \Omega^{(n)}$ the set of all Boolean functions.

A variable x_i is an *essential* variable of f if f *depends* on its i -th argument, that is if there are $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n \in \{0, 1\}$ such that the unary function $f(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n)$ is nonconstant. By *essential arity* of a function $f \in \Omega^{(n)}$, denoted $\text{ess } f$, we simply mean the number of its essential variables. For instance, constant functions are exactly those functions with essential arity 0. Functions with essential arity 1 are either projections or negated projections.

2.1. Simple minors and irreducible Boolean functions. A Boolean function $g \in \Omega^{(m)}$ is said to be a *simple minor* of a Boolean function $f \in \Omega^{(n)}$ if

there is a mapping $\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, m\}$ such that

$$g = f(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

If σ is not injective, then we speak of *identification of variables*. If σ is not surjective, then we speak of *addition of inessential variables*. If σ is a bijection, then we speak of *permutation of variables*. In fact, these Mal'cev operations are sufficient to completely describe the simple minor relation.

Fact 1. *The simple minor relation between Boolean functions is a quasi-order.*

Let \leq denote the simple minor relation on the set Ω of all Boolean functions. If $g \leq f$ and $f \leq g$, then we say that f and g are *equivalent*, denoted $f \equiv g$. The equivalence class of f is denoted by \tilde{f} . If $g \leq f$ but $f \not\leq g$, then we use the notation $g < f$. The arity gap of f , denoted $\text{gap } f$, is defined by $\text{gap } f = \min\{\text{ess } f - \text{ess } g : g < f\}$. Note that equivalent functions may differ in arity, but not in essential arity nor in arity gap.

Fact 2. *If $g \leq f$, then $\text{ess } g \leq \text{ess } f$, with equality if and only if $g \equiv f$.*

Let $(\tilde{\Omega}, \sqsubseteq)$ denote the poset made of equivalence classes of Boolean functions associated with the simple minor relation, that is, $\tilde{\Omega} = \Omega / \equiv$ together with the partial order \sqsubseteq given by $\tilde{g} \sqsubseteq \tilde{f}$ if and only if $g \leq f$. Several properties of this poset were established in [7]. For example, Fact 2 implies that each principal initial segment $\downarrow \tilde{f} = \{\tilde{g} : \tilde{g} \sqsubseteq \tilde{f}\}$ is finite. This means that $(\tilde{\Omega}, \sqsubseteq)$ decomposes into levels $\tilde{\Omega}_0, \dots, \tilde{\Omega}_n, \dots$, where $\tilde{\Omega}_n$ is the set of minimal elements of $\tilde{\Omega} \setminus \bigcup\{\tilde{\Omega}_m : m < n\}$.

Fact 3. *If $\text{ess } g = n$ and \tilde{g} is covered by \tilde{f} , then $\text{ess } f = n + \text{gap } f$.*

This fact and Salomaa's result [22] which asserts that the arity gap of Boolean functions is at most 2, imply that each level of $(\tilde{\Omega}, \sqsubseteq)$ is finite. For instance, the first level $\tilde{\Omega}_0$ comprises four equivalence classes, namely, those of constant 0 and 1 functions, and those of projections and negated projections. These four classes induce a partition of $(\tilde{\Omega}, \sqsubseteq)$ into four different blocks with no comparabilities in between them. For further background see [7].

We say that Boolean function f is *irreducible* if there is $f' \in \Omega$ such that

- (i) $f' < f$, and
- (ii) for every $g \in \Omega$, if $g < f$, then $g \leq f'$.

Fact 4. *A Boolean function f is irreducible if and only if \tilde{f} has a unique lower cover, i.e., \tilde{f} is join-irreducible in $(\tilde{\Omega}, \sqsubseteq)$.*

To illustrate, consider the binary conjunction $x_1 \wedge x_2$, the binary disjunction $x_1 \vee x_2$ and the composite $(x_1 \vee x_2) \wedge (x_3 \vee x_4)$. Both the binary conjunction and disjunction constitute irreducible functions since they have, up to equivalence, a unique strict minor, namely, a projection. This uniqueness clearly extends to any conjunction and disjunction of $n \geq 2$ variables, showing that any of the latter functions also constitute irreducible functions. But this is not the case for the composite $(x_1 \vee x_2) \wedge (x_3 \vee x_4)$. Indeed, $x_1 \wedge x_3 \vee x_1 \wedge x_4, x_1 \wedge x_4 \vee x_2 \leq (x_1 \vee x_2) \wedge (x_3 \vee x_4)$, but $x_1 \wedge x_3 \vee x_1 \wedge x_4 \not\equiv x_1 \wedge x_4 \vee x_2$. These observations lead to the following problem.

Problem 1. *Describe the irreducible Boolean functions.*

2.2. Boolean functions as polynomials. In this subsection, we view $\{0, 1\}$ as endowed with the two-element field structure, $\{0, 1\} = GF(2)$, as well as with the lattice structure where $0 < 1$. Consider the commutative ring $GF(2)[x_1, \dots, x_n]$ of multilinear polynomials in n indeterminates. Each of these polynomials is characterized by the fact that each monomial is a product of distinct indeterminates.

To each polynomial $P \in GF(2)[x_1, \dots, x_n]$ corresponds an n -ary Boolean function $f_P: \{0, 1\}^n \rightarrow \{0, 1\}$ which is given as the evaluation of P , that is, for every $(a_1, \dots, a_n) \in \{0, 1\}^n$, $f_P(a_1, \dots, a_n) = P(a_1, \dots, a_n)$. The function f_P is said to be *represented* by P , and P is said to be *Zhegalkin* (or *Reed-Muller*) polynomial of f_P [18, 21, 23]. As it is well-known every Boolean function can be represented in this way.

Theorem 5. *Every Boolean function $f: \{0, 1\}^n \rightarrow \{0, 1\}$, $n \geq 1$, is uniquely represented by a multilinear polynomial $P \in GF(2)[x_1, \dots, x_n]$.*

This result allows to work with polynomials rather than Boolean functions. This approach turns out to be quite useful when studying the poset $(\tilde{\Omega}, \sqsubseteq)$. For instance, as we mentioned the four equivalence classes in $\tilde{\Omega}_0$, namely, those represented by $0, 1, x_1$ and $x_1 + 1$ induce a partition of $\tilde{\Omega}$ into different blocks with no comparabilities in between them. As it is easy to verify, above the equivalence classes represented by the constant polynomials 0 or 1 we have the equivalence classes of those functions whose Zhegalkin polynomials are the sum of an even number of nonconstant monomials plus 0 or 1, respectively, and above the equivalence classes represented by x_1 or $x_1 + 1$ we have the equivalence classes of those functions whose Zhegalkin polynomials are the sum of an odd number of nonconstant monomials plus 0 or 1, respectively.

Corollary 6. *A variable x_i is essential in $f \in \Omega^{(n)}$ if and only if x_i appears in the Zhegalkin polynomial of f . In particular, $\text{ess } f$ is the number of variables appearing in the Zhegalkin polynomial of f .*

Thus, in the case of polynomial expressions, to describe the simple minor relation we only need to consider identification and permutation of essential variables, since the operation of addition of inessential variables produces the same polynomial representations. Moreover, from Fact 2 it follows that the strict minors of a given function f have Zhegalkin polynomials with strictly less variables, and that the Zhegalkin polynomials of functions equivalent to f are obtained from the Zhegalkin polynomial of f by permutation of its variables. For further developments see [6].

We finish this section with a complete classification of Boolean functions according to their arity gap, and which we shall make use of in the following sections.

Theorem 7. (In [4]:) *Let $f: \{0, 1\}^n \rightarrow \{0, 1\}$ be a Boolean function with at least two essential variables. Then the arity gap of f is two if and only if its Zhegalkin polynomial is equivalent to one of the following:*

- (1) $x_1 + x_2 + \dots + x_m + c$ for some $m \geq 2$,
- (2) $x_1 x_2 + x_1 + c$,
- (3) $x_1 x_2 + x_1 x_3 + x_2 x_3 + c$,
- (4) $x_1 x_2 + x_1 x_3 + x_2 x_3 + x_1 + x_2 + c$,

where $c \in \{0, 1\}$. Otherwise the arity gap of f is one.

3. BOOLEAN FUNCTIONS AND HYPERGRAPHS

By an *hypergraph* we simply mean a pair $\mathcal{H} = (V, \mathcal{E})$ where V is a finite nonempty set whose elements are called *vertices*, and where \mathcal{E} is a collection of

subsets of V called *hyperedges*. If V has n elements, then we set $V = \{1, \dots, n\}$ and we write $[V]^m$ to denote the set of m -element subsets of V .

Let $\mathcal{H} = (V, \mathcal{E})$ be an hypergraph with n vertices. To such an hypergraph \mathcal{H} we associate a polynomial $P_{\mathcal{H}} \in GF(2)[x_i, i \in V]$ which is given by $P_{\mathcal{H}} = \sum_{E \in \mathcal{E}} \prod_{i \in E} x_i$.

Example 1. Let $\mathcal{H}_1 = (\{1, 2, 3\}, \emptyset)$, $\mathcal{H}_2 = (\{1, 2, 3\}, \{\{1, 2\}, \emptyset\})$ and $\mathcal{H}_3 = (\{1, 2, 3\}, \{\{1, 2\}, \{1, 3\}, \{2, 3\}\})$. Then $\mathcal{P}_{\mathcal{H}_1} = 0$, $\mathcal{P}_{\mathcal{H}_2} = x_1x_2 + 1$ and $\mathcal{P}_{\mathcal{H}_3} = x_1x_2 + x_1x_3 + x_2x_3$, respectively.

Conversely, it is clear that to each polynomial $P \in GF(2)[x_1, \dots, x_n]$ is associated an hypergraph $\mathcal{H}_P = (V, \mathcal{E})$ where $V = \{1, \dots, n\}$ and \mathcal{E} is the set of hyperedges corresponding to the monomials of P . Thus, using the two-way correspondence between Boolean functions and polynomials over $GF(2)$, we have the following.

Theorem 8. *For each Boolean function $f: \{0, 1\}^n \rightarrow \{0, 1\}$, $n \geq 1$, there is a unique hypergraph $\mathcal{H} = (V, \mathcal{E})$, $V = \{1, \dots, n\}$, such that $f = f_{P_{\mathcal{H}}}$.*

For the sake of simplicity, let $f_{\mathcal{H}}$ denote the function $f_{P_{\mathcal{H}}}$ determined by \mathcal{H} .

3.1. Simple minors of hypergraphs. Let $\mathcal{H} = (V, \mathcal{E})$ and $\mathcal{H}' = (V', \mathcal{E}')$ be two hypergraphs and let $h': V' \rightarrow V$ be a map. For each $E \subseteq V$, set $h'^{-1}[E] = \{E' \in \mathcal{E}' : h'(E') = E\}$, where $h'(E') = \{h'(i') : i' \in E'\}$. The map h' is said to be a *quotient map from \mathcal{H}' to \mathcal{H}* , denoted $h': \mathcal{H}' \rightarrow \mathcal{H}$, if for every $E \subseteq V$, the following condition holds: $E \in \mathcal{E}$ if and only if the cardinality $|h'^{-1}[E]|$ is odd. We say that an hypergraph \mathcal{H} is a *simple minor* of an hypergraph \mathcal{H}' , denoted $\mathcal{H} \preceq \mathcal{H}'$, if there is a quotient map from \mathcal{H}' to \mathcal{H} .

To illustrate, let $\mathcal{H} = (V, \mathcal{E})$ be an hypergraph with $V = \{1, \dots, n\}$. Let $e = \{i, j\}$, $i, j \in V$, and fix $l_e \notin V$. Consider the hypergraph $\mathcal{H}_e = (V_e, \mathcal{E}_e)$ given as follows: $V_e = (V \setminus e) \cup \{l_e\}$ and for each $E \subseteq V_e$, we have $E \in \mathcal{E}_e$ if either

- (i) $E \in \mathcal{E}$ and $e \cap E = \emptyset$, or
- (ii) $l_e \in E$ and among $(E \setminus \{l_e\}) \cup e$, $(E \setminus \{l_e\}) \cup \{i\}$ and $(E \setminus \{l_e\}) \cup \{j\}$, either one or the three sets belong to \mathcal{E} .

Note that the condition (ii) guarantees that the map $h: V \rightarrow V_e$ defined by $h(i) = h(j) = l_e$ and $h(k) = k$, for each $k \neq i, j$, constitutes a quotient map from \mathcal{H} to \mathcal{H}_e , thus showing that \mathcal{H}_e is a simple minor of \mathcal{H} .

Lemma 9. *The simple minor relation between hypergraphs is a quasi-order.*

Proof. Let $\mathcal{H} = (V, \mathcal{E})$, $\mathcal{H}' = (V', \mathcal{E}')$ and $\mathcal{H}'' = (V'', \mathcal{E}'')$ be hypergraphs such that $\mathcal{H} \preceq \mathcal{H}' \preceq \mathcal{H}''$. Let $h': \mathcal{H}' \rightarrow \mathcal{H}$ and $h'': \mathcal{H}'' \rightarrow \mathcal{H}'$ be the corresponding quotient maps. We claim that $h = h' \circ h''$ is a quotient map from \mathcal{H}'' to \mathcal{H} .

Let $E \subseteq V$. The set $h^{-1}[E] = \{E'' \in \mathcal{E}'' : h''(E'') = E\}$ decomposes into two sets, namely, $A = \bigcup \{h''^{-1}[E'] : E' \in \mathcal{E}', h'(E') = E\}$ and $B = \bigcup \{h''^{-1}[E'] : E' \notin \mathcal{E}', h'(E') = E\}$. Now A is a disjoint union of sets of odd size and B is a disjoint union of sets of even size and hence, B has even size. Thus the parity of $|h^{-1}[E]|$ is the same as the parity of $|A|$ which, in turn, is the same as the parity of $|h'^{-1}[E]|$. Since $E \in \mathcal{E}$ if and only if $|h'^{-1}[E]|$ is odd, the proof is now complete. \square

The following theorem establishes the connection between the simple minor relation on Boolean functions and the simple minor relation on hypergraphs.

Theorem 10. *Let $\mathcal{H} = (V, \mathcal{E})$ and $\mathcal{H}' = (V', \mathcal{E}')$ be two hypergraphs, with $V = \{1, \dots, n\}$ and $V' = \{1, \dots, m\}$, respectively. Then $\mathcal{H} \preceq \mathcal{H}'$ if and only if $f_{\mathcal{H}} \leq f_{\mathcal{H}'}$.*

Proof. Suppose first that $\mathcal{H} \preceq \mathcal{H}'$ and let $h': \mathcal{H}' \rightarrow \mathcal{H}$ be the quotient map. Define $\sigma: \{1, \dots, m\} \rightarrow \{1, \dots, n\}$ by $\sigma(i') = h(i')$, for every $i' \in V' = \{1, \dots, m\}$. To verify $f_{\mathcal{H}} \leq f_{\mathcal{H}'}$, we only have to show that $P_{\mathcal{H}} = P_{\mathcal{H}'}(x_{\sigma(1)}, \dots, x_{\sigma(m)})$. Indeed,

$$P_{\mathcal{H}'}(x_{\sigma(1)}, \dots, x_{\sigma(m)}) = \sum_{E' \in \mathcal{E}'} \prod_{i' \in E'} x_{\sigma(i')} = \sum_{E' \in \mathcal{E}'} \prod_{i' \in E'} x_{h(i')} = \sum_{E' \in \mathcal{E}'} \prod_{i \in h'(E')} x_i^{|h'^{-1}(i)|}.$$

Since $x_j^2 = x_j$, we have that $\prod_{i \in h'(E')} x_i^{|h'^{-1}(i)|} = \prod_{i \in h'(E')} x_i$. Hence,

$$P_{\mathcal{H}'}(x_{\sigma(1)}, \dots, x_{\sigma(m)}) = \sum_{E \subseteq V} \sum_{h'(E')=E} \prod_{i \in h'(E')} x_i.$$

Now each term $\sum_{h'(E')=E} \prod_{i \in h'(E')} x_i$ is different to 0 if and only if $|h'^{-1}[E]|$ is odd, that is, $E \in \mathcal{E}$. In other words, $P_{\mathcal{H}'}(x_{\sigma(1)}, \dots, x_{\sigma(m)}) = P_{\mathcal{H}}$.

Now suppose that $f_{\mathcal{H}} \leq f_{\mathcal{H}'}$ and let $\sigma: \{1, \dots, m\} \rightarrow \{1, \dots, n\}$ be a map such that $P_{\mathcal{H}} = P_{\mathcal{H}'}(x_{\sigma(1)}, \dots, x_{\sigma(m)})$. Define $h': V' \rightarrow V$ by $h(i') = \sigma(i')$, for every $i' \in V' = \{1, \dots, m\}$. Let $E \subseteq V$. We have that $E \in \mathcal{E}$ if and only if $\prod_{i \in E} x_i$ is a monomial of $P_{\mathcal{H}}$. Since $P_{\mathcal{H}} = P_{\mathcal{H}'}(x_{\sigma(1)}, \dots, x_{\sigma(m)})$, the latter condition holds if and only if the number of monomials $\prod_{i' \in E'} x_{i'}$ of $P_{\mathcal{H}'}$ such that $\sigma(E') = E$ is odd. In other words, $E \in \mathcal{E}$ if and only if $|h'^{-1}[E]|$ is odd. This shows that h' constitutes a quotient map from \mathcal{H}' to \mathcal{H} . \square

3.2. Conditions for irreducibility. Let $\mathcal{H} = (V, \mathcal{E})$ and $\mathcal{H}' = (V', \mathcal{E}')$ be two hypergraphs. A map $\varphi: V \rightarrow V'$ is said to be an *isomorphism* from \mathcal{H} onto \mathcal{H}' if φ is bijective and for every $E \subseteq V$, $E \in \mathcal{E}$ if and only if $\varphi(E) \in \mathcal{E}'$. Two hypergraphs \mathcal{H} and \mathcal{H}' are said to be *isomorphic*, denoted $\mathcal{H} \cong \mathcal{H}'$, if there is an isomorphism φ from \mathcal{H} onto \mathcal{H}' . If $\mathcal{H} = \mathcal{H}'$, then φ is called an *automorphism* of \mathcal{H} . The group made of automorphisms of \mathcal{H} is denoted by $\text{Aut}(\mathcal{H})$.

Let $\mathcal{H} = (V, \mathcal{E})$ be an hypergraph and let $\overline{V} = \bigcup \mathcal{E}$. For $e, e' \in [\overline{V}]^2$, define $e \approx e'$ if $\mathcal{H}_e \cong \mathcal{H}_{e'}$. Obviously, \approx is an equivalence relation.

Lemma 11. *Let $\mathcal{H} = (V, \mathcal{E})$ be an hypergraph. Then $f_{\mathcal{H}}$ is irreducible if and only if $|\overline{V}| \geq 2$ and there is an equivalence class \mathcal{C} of \approx such that, for every $e' \in [\overline{V}]^2 \setminus \mathcal{C}$ and $e \in \mathcal{C}$, $\text{ess } f_{\mathcal{H}_{e'}} < \text{ess } f_{\mathcal{H}_e}$.*

In the search for hypergraphs $\mathcal{H} = (V, \mathcal{E})$ determining irreducible Boolean functions, Lemma 11 invites us to look at differences $\text{ess } f_{\mathcal{G}} - \text{ess } f_{\mathcal{G}_e}$, especially, when $\text{ess } f_{\mathcal{G}} - \text{ess } f_{\mathcal{G}_e} > 1$. For the latter to occur, there are two possibilities:

- (i) the vertex l_e becomes isolated and this is the case if and only if, for every F disjoint from e , the number of $e' \subseteq V$ such that $\emptyset \neq e' \subseteq e$ and $e' \cup F \in \mathcal{E}$, is even, or
- (ii) another vertex, say $i \in V$, becomes isolated and this is the case if and only if, for every $e' \in \mathcal{E}$, if $i \in e'$ then $e \cap e' \neq \emptyset$ and there is $e'' \in \mathcal{E}$ such that $i \in e''$ and $e' \setminus e = e'' \setminus e$.

Note that if $\text{ess } f_{\mathcal{G}} - \text{ess } f_{\mathcal{G}_e} > 1$, for every $e \in [V]^2$, then by Theorem 7 it follows that $\text{ess } f_{\mathcal{G}} - \text{ess } f_{\mathcal{G}_e} = 2$, for every $e \in [V]^2$, and \mathcal{G} determines a function which is equivalent to one listed in Theorem 7.

As an immediate consequence of Lemma 11, we get the following criterion for irreducibility.

Corollary 12. *Let $\mathcal{H} = (V, \mathcal{E})$ be an hypergraph. If $|\overline{V}| \geq 2$ and, for every $e, e' \in [\overline{V}]^2$, we have $e \approx e'$, then $f_{\mathcal{H}}$ is irreducible.*

A group G acting on a set V is *2-set transitive* if for every $e, e' \in [V]^2$, there is some $g \in G$ such that $g(e) = e'$.

Corollary 13. *Let $\mathcal{H} = (V, \mathcal{E})$ be an hypergraph. If $|V| \geq 2$, $\bigcup \mathcal{E} = V$ and $\text{Aut}(\mathcal{H})$ is 2-set transitive, then $f_{\mathcal{H}}$ is irreducible.*

Proof. Let $\varphi \in \text{Aut}(\mathcal{H})$. Take $e \in [V]^2$ and let $e' = \varphi(e) \in [V]^2$. Consider the mapping $\overline{\varphi} : V_e \rightarrow V_{e'}$ defined by $\overline{\varphi}(l_e) = l_{e'}$ and $\overline{\varphi}(i) = i$ for every $i \in V_e \setminus \{l_e\}$. Clearly, $\overline{\varphi}$ constitutes the desired isomorphism from \mathcal{H}_e to $\mathcal{H}_{e'}$. \square

Problem 2. *For which hypergraphs \mathcal{H}*

- (i) *$\text{Aut}(\mathcal{H})$ is 2-set transitive?*
- (ii) *$\mathcal{H}_e \cong \mathcal{H}_{e'}$, for every $e, e' \in [V]^2$?*

Examples are given in the next subsection.

3.3. Steiner Systems. Let $\mathcal{H} = (V, \mathcal{E})$ be an hypergraph. We say that the hypergraph \mathcal{H} is a *2- (n, k, λ) design* if $|V| = n$, $\mathcal{E} \subseteq [V]^k$, and for every $e \in [V]^2$, $|\{E \in \mathcal{E} : e \subseteq E\}| = \lambda$. If $\lambda = 1$, then we say that \mathcal{H} is a *Steiner system* and, in addition, if $k = 3$, then we say that \mathcal{H} is a *Steiner triple system*.

For each $e \in [V]^2$, set $\mathcal{H}_{\setminus e} = (V \setminus e, \mathcal{E} \cap [V \setminus e]^2)$. If for every $e, e' \in [V]^2$, $\mathcal{H}_{\setminus e} \cong \mathcal{H}_{\setminus e'}$, then we say that \mathcal{H} is *-2-monomorphic*. The following theorem reveals a connection between the notion of -2-monomorphicity and irreducibility in the case of Steiner systems.

Theorem 14. *Let $\mathcal{H} = (V, \mathcal{E})$ be a Steiner system. The following are equivalent:*

- (i) *$f_{\mathcal{H}}$ is irreducible;*
- (ii) *$\mathcal{H}_e \cong \mathcal{H}_{e'}$, for every $e, e' \in [V]^2$;*
- (iii) *\mathcal{H} is -2-monomorphic.*

Problem 3. *For a Steiner triple system $\mathcal{H} = (V, \mathcal{E})$ does the following hold: \mathcal{H} is -2-monomorphic if and only if $\text{Aut}(\mathcal{H})$ is 2-set transitive?*

Note that the automorphism group of a Steiner systems is flag-transitive whenever it is 2-set transitive. The converse holds for Steiner triple systems. There are several deep results about Steiner systems with a 2-transitive or a flag transitive automorphism group (see the survey by Kantor [16]). For example, any Steiner triple system with a 2-transitive automorphism group must be a projective space over $GF(2)$ or an affine space over $GF(3)$ [14, 17]. The notion of monomorphy (with some of its variations) is due to R. Fraïssé. His book [12] contains some important results concerning this notion.

4. JOIN-IRREDUCIBLE GRAPHS

In this subsection, we give an answer to Problem 1 in the particular case of functions which are determined by simple graphs, that is graphs $\mathcal{G} = (V, \mathcal{E})$ where $\mathcal{E} \subseteq [V]^2$. As in the case of hypergraphs, if we remove the isolated vertices of \mathcal{G} , the resulting graph $\tilde{\mathcal{G}}$ yields an equivalent function. In the sequel, when we speak of a *join-irreducible* graph we simply mean a graph \mathcal{G} such that $\tilde{\mathcal{G}}$ is join-irreducible. Note that \mathcal{G} is join-irreducible if and only if $\tilde{\mathcal{G}}$ is join-irreducible; note also that a join-irreducible graph must have at least one edge.

Given a graph $\mathcal{G} = (V, \mathcal{E})$, we write $i \sim j$ if $\{i, j\} \in \mathcal{E}$. Set $V(i) = \{j \in V : i \sim j\} \cup \{i\}$. The *degree* of a vertex i , denoted $d(i)$, is the cardinality $|V(i)| - 1$. For example, in the *complete* graph K_n each vertex has degree $n - 1$, while in a *cycle* C_n each vertex has degree 2. The graph \mathcal{G} is said to be *connected* if any

two vertices of \mathcal{G} are connected by a path. We denote by $\overline{\mathcal{G}}$ the *complement* of \mathcal{G} , that is, $\overline{\mathcal{G}} = (V, [V]^2 \setminus \mathcal{E})$. The *disjoint union* of two graphs $\mathcal{G}_1 = (V_1, \mathcal{E}_1)$, $\mathcal{G}_2 = (V_2, \mathcal{E}_2)$, $V_1 \cap V_2 = \emptyset$, is defined as the graph $\mathcal{G} = (V_1 \cup V_2, \mathcal{E}_1 \cup \mathcal{E}_2)$. The *graph join* of $\mathcal{G}_1 = (V_1, \mathcal{E}_1)$ and $\mathcal{G}_2 = (V_2, \mathcal{E}_2)$, denoted $\mathcal{G}_1 + \mathcal{G}_2$, is defined as the disjoint union of \mathcal{G}_1 and \mathcal{G}_2 together with the edges $\{i_1, i_2\}$ for all $i_1 \in V_1$ and $i_2 \in V_2$. For further background in graph theory, see e.g. [1, 8, 13].

The proofs of the following results are omitted and can be verified by repeated use of Lemma 11. To illustrate we provide a proof of Proposition 15 which settles the case of disconnected graphs.

Proposition 15. *Suppose \mathcal{G} is disconnected. Then \mathcal{G} is join-irreducible if and only if $\check{\mathcal{G}}$ is isomorphic to the disjoint union of n copies of K_3 , for some $n \geq 2$.*

Proof. Clearly, if $\check{\mathcal{G}}$ is isomorphic to the disjoint union of n copies of K_3 , for some $n \geq 2$, then \mathcal{G} is join-irreducible. For the converse, we may suppose with no loss of generality that $\mathcal{G} = \check{\mathcal{G}}$. Let \mathcal{G}_1 and \mathcal{G}_2 be two connected components of \mathcal{G} . Note that $|\mathcal{G}_1|, |\mathcal{G}_2| \geq 2$. Take $i \in \mathcal{G}_1$ and $j \in \mathcal{G}_2$, and let $e = \{i, j\}$. Clearly, $|\mathcal{G}_e| = |\mathcal{G}| - 1$, no vertex is isolated in \mathcal{G}_e and \mathcal{G}_e has one less connected component than \mathcal{G} .

Now take $i, i' \in \mathcal{G}_1$ and let $e' = \{i, i'\}$. Clearly, for every such choice of e' , we have $e \not\approx e'$. Since \mathcal{G} is join-irreducible, Lemma 11 implies that $\text{ess } f_{\mathcal{G}_{e'}} < \text{ess } f_{\mathcal{G}_e}$. In other words, for every $e' = \{i, i'\}$, $i, i' \in \mathcal{G}_1$, $\text{ess } f_{\mathcal{G}_{e'}} \leq \text{ess } f_{\mathcal{G}} - 2$. From Theorem 7 it follows that \mathcal{G}_1 must be isomorphic to K_3 . Since the choice of connected components was arbitrary, we conclude that \mathcal{G} is isomorphic to the disjoint union of n copies of K_3 , for some $n \geq 2$. \square

To deal with the case of connected graphs, we need to introduce some terminology. Let $\mathcal{G} = (V, \mathcal{E})$ be a graph. A subset $S \subseteq V$ is said to be *autonomous* if for every $i, i' \in S$ and $j \in V \setminus S$, $i \sim j$ if and only if $i' \sim j$. Moreover, S is said to be *independent* if for every $i, i' \in S$, $i \not\sim i'$. For simplicity, we refer to autonomous independent sets as *ai-sets*. We say that \mathcal{G} is *ai-prime* if its *ai-sets* are empty or singletons.

Fact 16. *For each $i \in V$, the union of all ai-sets containing i is an ai-set called the ai-component of i . Moreover, each graph \mathcal{G} decomposes into ai-components.*

On the set of ai-components of \mathcal{G} there is a graph structure, denoted \mathcal{G}_{ai} , in such a way that \mathcal{G} is the lexicographic sum of its ai-components and indexed by \mathcal{G}_{ai} . Note that the graph \mathcal{G}_{ai} is ai-prime.

These constructions are variants of the classical notions of decomposition of graphs and prime graphs (see [9]).

Lemma 17. *Let $\mathcal{G} = (V, \mathcal{E})$ be a connected graph and suppose that there is $e \in [V]^2 \setminus \mathcal{E}$ such that \mathcal{G}_e has no isolated vertices. Then there is $e' \in \mathcal{E}$ such that $\mathcal{G}_{e'}$ has no isolated vertices.*

Thus, if $\mathcal{G} = (V, \mathcal{E})$ is join-irreducible, \mathcal{G}_e has an isolated vertex for every $e \in [V]^2 \setminus \mathcal{E}$. Moreover, the nonedge $e = \{i_1, i_2\} \in [V]^2 \setminus \mathcal{E}$ must be in a ai-component or there is $j \in V$ such that $d(j) = 2$ and $i_1 \sim j \sim i_2$.

We say that a graph $\mathcal{G} = (V, \mathcal{E})$ *satisfies (P)* if for every nonedge $e = \{i_1, i_2\} \in [V]^2 \setminus \mathcal{E}$ there is $j \in V$ such that $d(j) = 2$ and $i_1 \sim j \sim i_2$.

Lemma 17 and the observation above yield the following.

Corollary 18. *If a connected graph \mathcal{G} is join-irreducible, then \mathcal{G}_{ai} satisfies (P).*

Our next proposition describes those graphs satisfying property (P).

Proposition 19. *A graph $\mathcal{G} = (V, \mathcal{E})$ satisfies (P) if and only if \mathcal{G} is either isomorphic to K_n , for some $n \geq 2$, C_5 , C_4 or to a 3-element path.*

Sketch proof. We observe that each member of the list satisfies (P). Conversely, suppose that $\mathcal{G} = (V, \mathcal{E})$ satisfies (P). We prove successively:

Claim 1. Let $e = \{i_1, i_2\} \in [V]^2 \setminus \mathcal{E}$ and $j \in V$ such that $d(j) = 2$ and $i_1 \sim j \sim i_2$. If $e' := \{j, j'\} \in [V]^2 \setminus \mathcal{E}$ then either $e_1 := \{i_1, j'\} \in \mathcal{E}$ and $d(i_1) = 2$ or $e_2 := \{i_2, j'\} \in \mathcal{E}$ and $d(i_2) = 2$.

Claim 2. Let $i \in V$. If $d(i) \geq 3$, then $\mathcal{G}(i) = (V(i), [V(i)]^2 \cap \mathcal{E})$ is isomorphic to K_n , for some $n \geq 2$. In fact, $\mathcal{G}(i) = \mathcal{G}$.

According to Claim 2, if \mathcal{G} is not isomorphic to K_n , the degree of each vertex is at most 2. Since \mathcal{G} satisfies (P), it must be isomorphic to one of the three last members of our list. \square

As a corollary we get the following result.

Corollary 20. *If \mathcal{G} is connected and join-irreducible, then \mathcal{G}_{ai} is isomorphic to K_n , for some $n \geq 2$, or to C_5 .*

Clearly, each K_n , $n \geq 2$, and C_5 are join-irreducible graphs. Thus, if $\mathcal{G} = (V, \mathcal{E})$ is an *ai*-prime graph, then \mathcal{G} is join-irreducible if and only if \mathcal{G} is isomorphic to K_n , for some $n \geq 2$, or to C_5 .

Now if a connected and join-irreducible graph $\mathcal{G} = (V, \mathcal{E})$ is not an *ai*-prime graph, then \mathcal{G}_{ai} cannot be isomorphic to C_5 . Indeed, for the sake of contradiction, suppose that \mathcal{G}_{ai} is isomorphic to C_5 . Let $\mathcal{G}_1, \dots, \mathcal{G}_5$ be the *ai*-components of \mathcal{G} such that \mathcal{G}_i is connected to \mathcal{G}_{i+1} , for $i = 1, 2, 3, 4$ and \mathcal{G}_5 is connected to \mathcal{G}_1 . Assume, without loss of generality, that $|\mathcal{G}_1| \geq 2$. Consider $i, i' \in \mathcal{G}_1$, $i_2 \in \mathcal{G}_2$ and $i_3 \in \mathcal{G}_3$, and let $e = \{i, i_2\}$ and $e' = \{i', i_3\}$. Clearly, $e \not\approx e'$ and $\text{ess } f_{\mathcal{G}_e} = \text{ess } f_{\mathcal{G}_{e'}}$. By Lemma 11 it follows that \mathcal{G} is not join-irreducible which constitutes the desired contradiction. Thus, by Corollary 20 it follows that, in the non *ai*-prime case, if $\mathcal{G} = (V, \mathcal{E})$ is join-irreducible, then \mathcal{G}_{ai} is isomorphic to K_n , for some $n \geq 2$.

Proposition 21. *Let $\mathcal{G} = (V, \mathcal{E})$ be a connected and non *ai*-prime graph. Then \mathcal{G} is join-irreducible if and only if \mathcal{G} is isomorphic to one of the following graphs:*

- (i) $K_2 + \overline{K}_m$, for some $m \geq 2$;
- (ii) $\overline{K}_n + \overline{K}_m$, for some n, m with $1 \leq n < m$;
- (iii) a graph join $\overline{K}_n + \dots + \overline{K}_n$ of r copies of K_n , for some $r, n \geq 2$.

Sketch proof. As observed if $\mathcal{G} = (V, \mathcal{E})$ is join-irreducible, then \mathcal{G}_{ai} is isomorphic to K_r , for some $r \geq 2$. For $r = 2$, it is clear that \mathcal{G} is isomorphic to $\overline{K}_n + \overline{K}_m$ for some $n, m \geq 1$. For $r = 3$, if there is $i \in V$ such that $d(i) = 2$, then we show that \mathcal{G} is isomorphic to $K_2 + \overline{K}_m$, for some $m \geq 2$. If $r \geq 3$ and for every $i \in V$ we have $d(i) > 2$, then we show that \mathcal{G} is the join $\overline{K}_n + \dots + \overline{K}_n$ of r copies of K_n for some $n \geq 2$. \square

From these results, we obtain the description of the join-irreducible graphs.

Theorem 22. *Let $\mathcal{G} = (V, \mathcal{E})$ be a graph. Then \mathcal{G} is irreducible if and only if $\check{\mathcal{G}}$ is isomorphic to one of the following graphs:*

- (i) a disjoint union of n copies of K_3 , for some $n \geq 2$;
- (ii) C_5 ;
- (iii) $K_2 + \overline{K}_m$, for some $m \geq 2$;
- (iv) K_n , for some $n \geq 2$;
- (v) $\overline{K}_n + \overline{K}_m$, for some n, m with $1 \leq n < m$;
- (vi) a graph join $\overline{K}_n + \dots + \overline{K}_n$ of r copies of K_n , for some $r, n \geq 2$.

REFERENCES

- [1] A. BONDY, U.S.R. MURTY, Graph Theory, Series: Graduate Texts in Mathematics , Vol. 244 2008, XII, 652 p. 235 illus.
- [2] M. COUCEIRO, S. FOLDES, On closed sets of relational constraints and classes of functions closed under variable substitutions, *Algebra Universalis*, **54** (2005) 149–165.
- [3] M. COUCEIRO, S. FOLDES, Functional equations, constraints, definability of function classes, and functions of Boolean variables, *Acta Cybernet.* **18** (2007) 61–75.
- [4] M. COUCEIRO, E. LEHTONEN, On the effect of variable identification on the essential arity of functions on finite sets, *Int. J. Found. Comput. Sci.* **18** (2007) 975–986.
- [5] M. COUCEIRO, E. LEHTONEN, Generalizations of Świerczkowski’s lemma and the arity gap of finite functions, arXiv:0712.1753v1.
- [6] M. COUCEIRO, E. LEHTONEN, On the arity gap of finite functions: results and applications, manuscript submitted to ROGICS’08.
- [7] M. COUCEIRO, M. POUZET, On a quasi-ordering on Boolean functions, arXiv:math.CO/0601218, 2006.
- [8] R. DIESTEL, Graph Theory. Third Edition. Springer-Verlag, Heidelberg Graduate Texts in Mathematics, Volume 173, 2005
- [9] A. EHRENFUCHT, T. HARJU AND G. ROZENBERG, The theory of 2-structures. A framework for decomposition and transformation of graphs, World Scientific, 1999.
- [10] O. EKIN, S. FOLDES, P. L. HAMMER, L. HELLERSTEIN, Equational characterizations of Boolean function classes, *Discrete Math.* **211** (2000) 27–51.
- [11] S. FOLDES, G. POGOSYAN, Post classes characterized by functional terms, *Discrete Applied Mathematics* **142** (2004) 35–51.
- [12] R. FRAÏSSÉ, *Theory of relations*, second edition, North-Holland Publishing Co., Amsterdam, p.ii+451, 2000.
- [13] R.L. GRAHAM, M. GRÖTSCHEL, L. LOVASZ, (Editors), Handbook of Combinatorics vol. I, Elsevier, Amsterdam. The MIT Press, Cambridge, 1995.
- [14] M. HALL, JR., Steiner triple systems with doubly transitive automorphism group, *J. Comb. Theory (A)* **38**(1985) 192–202.
- [15] L. HELLERSTEIN, On generalized constraints and certificates, *Discrete Mathematics*, **226** (2001) 211–232.
- [16] W.M. KANTOR, 2-transitive and flag-transitive designs, *Coding theory, design theory, group theory (Burlington, VT, 1990)*, 13–30, Wiley-Intersci. Publ., Wiley, New-York, 1993.
- [17] J.D.KEY AND E.E.SHULT, Steiner triple systems with doubly transitive automorphism groups: A corollary of the classification theorem for the finite simple groups, *J. Comb. Theory (A)* **36**(1984) 105–110.
- [18] D. E. MULLER, Application of Boolean algebra to switching circuit design and to error correction, *IRE Trans. Electron. Comput.* **3**(3) (1954) 6–12.
- [19] N. PIPPENGER, Galois theory for minors of finite functions, *Discrete Math.* **254** (2002) 405–419.
- [20] G. POGOSYAN, Classes of Boolean functions defined by functional terms, *Multiple Valued Logic*, **7** (2002) 417–448.
- [21] I. S. REED, A class of multiple-error-correcting codes and the decoding scheme, *IRE Trans. Inf. Theory* **4**(4) (1954) 38–49.
- [22] A. SALOMAA, On essential variables of functions, especially in the algebra of logic, *Ann. Acad. Sci. Fenn. Ser. A I. Math.* **339** (1963) 3–11.
- [23] I. I. ZHEGALKIN, On the calculation of propositions in symbolic logic, *Mat. Sb.* **34** (1927) 9–28 (in Russian).

INSTITUT SUPÉRIEUR DES TECHNOLOGIES MÉDICALES DE TUNIS,, 9 AVENUE DR ZOUHAIR ESSAFI,, 1006 TUNIS, TUNISIE,

E-mail address: Moncef.Bouaziz@istmt.rnu.tn

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF LUXEMBOURG, 162A, AVENUE DE LA FAÏENCERIE, L-1511 LUXEMBOURG

E-mail address: miguel.couceiro@uni.lu

ICJ, DEPARTMENT OF MATHEMATICS, UNIVERSITÉ CLAUDE-BERNARD LYON1, 43 Bd 11 NOVEMBRE 1918, 68622 VILLEURBANNE CEDEX, FRANCE

E-mail address: pouzet@univ-lyon1.fr